ON THE SECURITY ANALYSIS OF AUTHENTICATION PROTOCOLS.

LUKA JOSHUA; ALIYU DANLADI HINA; & USMAN HASSAN[1].
Department of Mathematics & Statistics, the Federal Polytechnic, Bauchi, Bauchi State, Nigeria.

Abstract:
A logic for the analysis of authentication protocols was first proposed by Burrows, Abadi, and Needham (BAN). BAN logic is one of the formal protocol verification techniques that help us to prove whether a cryptographic protocol works correctly. It is a logic of belief, with special constructs for expressing some of the central concepts used in authentication. The logic has revealed many subtIeties and errors in published protocols that are hitherto considered secure. We considered a three-factor mutual authentication protocol based on multi-server environments who's underlyi ng security is build on cryptography. We analyze the protocol's security using informal security analysis, the BAN logic.

Keywords: Authentication protocols, BAN logic, cryptography, security analysis.

Introduction

In somany distribution systems, the basis of their security is the authentication protocols used. For the security to be extablished, the functions of the protocols will have to be analyzed. A simple logic has been developed which allowed us to describe the beliefs of trustworthy parties involved in authentication protocols and the evolution of these beliefs as a consequence of communication (Burrows, Abadi, & Needham, 1990; Harbi, Aliouat, Refoufi, Harous, & Bentaleb, 2019). Authentication is the process of determining the identity of a principal such as a computer, a server or a person, in a computer system. It plays the role of ensuring a secure system (Abadi & Tuttle, 1991). In a computer system, the principal that controls the resources in the system must have a way of identifying the identity of users wanting to use/access the resources in the system. This done through the use of individual access secrets like passwords and passcodes which are used as encryption keys. Each uer will be identified by his secret password. These secrets (passwords) have to be share across the principals so that each one will be uniquely identified. (Burrows et al., 1990; Abadi & Tuttle, 1991).

An authentication protocol is a description of how these secrets are distributed to principals, and how these secrets are used to determine principals' identities. An authentication protocol given below tries to establish a connection between three principals, the server (*S*), and two users (principals) *A* and *B* (Fakroon, Alshahrani, Gebali, & Traore, 2020). The server *S* is trusted to generate good encryption keys. The acquisition of a shared key that will enable *A* and *B* to communicate between themselves is the goal of the authentication protocol (Abadi & Tuttle, 1991; Ali et al., 2020). After authentication, two principals should be entitled to believe that they are communicating with each other and not with intruders.

For communications to be secure, many researchers have proposed di↵erent kinds of authentication protocols between client(s) and server(s). A user identification protocol based on public-key for the telecare medicine information systems had been proposed by (Ostad-Sharif, AbbasinezhadMood, & Nikooghadam, 2019). Mo et al. (Mo, Hu, Chen, & Shen, 2019) proposed an anonymous authentication protocol. They argued that their protocol was designed to have a reasonable computational cost for mobile devices with limited computational capability. A hash-based remote authentication protocol was proposed by(Zhang, Xie, & Ruan, 2019). This is to improve the e ciency of user authentication as claimed by them, even though it was found to be vulnerable to known session-specific temporary information attack because the session key consists of short-term key and public messages.

Multi-server-based authentication protocols that allow users to communicate with multiple servers have been proposed in the literature. A remote user authentication protocol for multiserver environments was proposed by (Hassan, Omala, Ali, Jin, & Li, 2019). It was however found to be weak against user anonimity by (Mwitende, Ali, Eltayieb, Wang, & Li, 2020). The authors in (Ying & Nayak, 2019) proposed a self-certified public key-based authentication protocol for 5G networks multi-server environments. It was reported to have been weak against user impersonation attack and does not ensure untraceability.

Despite all the e↵orts to come-up with state-of-the-art authentication protocols, most of them are always found to be vulnerable to one security problem or the other when deployed. These vulnerabilities cause critical security issues including leakages of personal information, data theft and governments' sensitive information. Thus, the need to subject proposed protocols to some kind of formal or informal security analysis is highly encouraged.

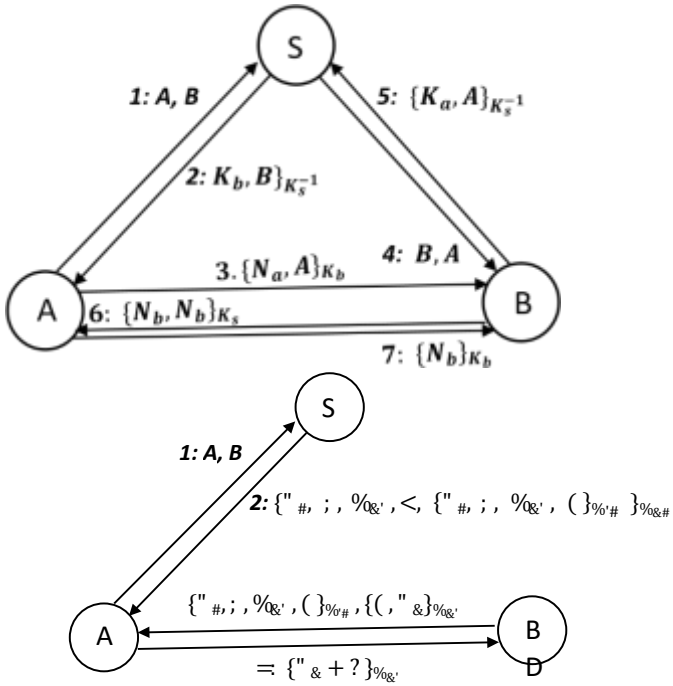
The Burrows-Abadi-Needham (BAN) logic is used to evaluate whether an authentication protocol works correctly. The BAN logic has been used to analyse a number of protocols which includes:

- **The Needham - Schroeder Protocol** (Figure 1a) is based on public-key cryptography; it allowed two principals to exchange two secret numbers.
- **The Kerberos protocol** (Figure 1b) establishes a shared key between two principals with help from an authentication server (Miller, Neuman, Schiller, & Saltzer, 1988; Burrows et al., 1990). It is based on the shared-key Needham- Schroeder protocol (Needham & Schroeder, 1978), one of the earliest protocols in use.
- **The Andrew Secure RPC Handshake** (Figure 1c) protocol uses an authentication handshake between two principals whenever a client binds to a new server. The handshake is intended to allow a client A to obtain a new session key $K_{ab}0$ from a server B, given that they already share a key K_{ab} (Satyanarayanan, 1989; Boonkrong, 2021).
- **The CCITT X.509 Protocol** (Figure 1d) is intended for a signed and secure communication between two principals, assuming that each knows the public key of the other.

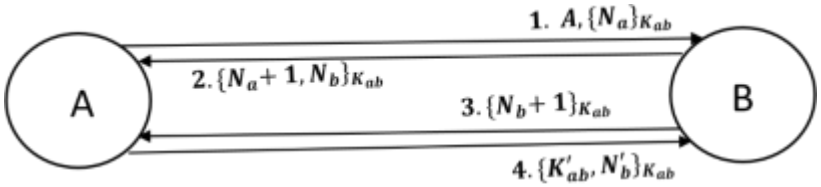
The BAN Logic

A formalism was built on many sorted model logic. In the logic we distinguish several sorts of objects: principals, encryption keys, and formulas (also called statements). We identify messages with statements in the logic. Typically, the symbols A, B, and S denote specific principals; K_{ab}, K,, and K_{bs} denote specific

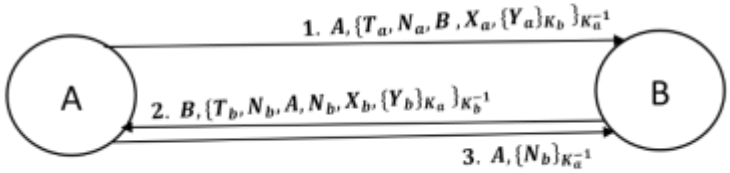
shared keys; K, K_b, and K_s denote specific public keys, and K_a^{-1}, K_b^{-1}, and K_s^{-1} denote the corresponding secret keys; and N, N_b, and N_c denote specific



(a) Needham - Schroeder Protocol (b) Kerberos Authentication Protocol



(c) The Andrew Square RPC Handshake Protocol



(d) The CCITT X. 509 Protocol.

Figure 1: Authentication Protocols
(Burrows et al., 1990)

statements (Burrows et al., 1990). The symbols P, Q, and R range over principals; X and Y range over statements; and K ranges over encryption keys.

The BAN (Burrows, Abadi, and Needham) logic is a formal security analysis proof used by many researchers to verify mutual authentication (Burrows et al., 1990). The BAN logic is a modal logic of belief. It has several modal operators including:

- $P \mid \Rightarrow X$: (P believes X) P is entitled to act as though X is true.
- A C X : (A sees X) someone has sent a message to A
- $A \mid \leftarrow\cdots K$ (A ponce said K) A used key K
- $A \mid \leftarrow\cdots X$: (A ponce said X) A uttered a message containing X.
- $A =) X$: (A has jurisdiction over X) A is an authority on X and can be trusted on X.
- $A \overset{K}{!} B$: (A and B share key K:) A and B can use key K to communicate. The key is unknown to anyone else.
- $\#X$: (X is fresh) meaning that X has not been sent before in any run of the protocol.
- $A \overset{K}{!} B$ (B has public key K) B has a published public key K and corresponding private key K^{-1}.
- $A \overset{X}{()} B$: (A and B share secret X) X is a secret known only to A, B and possibly some trusted associates.
- $\{X\}$ the formula X encrypted under the key K
- hXiY This represents X combined with the secret formula Y . The posession of Y proves the identity of whoever utters hXiY .

The BAN Logic Rules

There are numerous rules of inference for manipulating the protocol to generate a set of beliefs.

- **Message meaning (MM):** If A believes (A share(K) B) and A sees $\{X\}K$ then A believes(B said X).

$$\frac{A| \equiv (A \overset{K}{\rightarrow} B), A \lhd \{X\}_K}{A| \equiv (B| \sim X)} \quad (1)$$

- **Nonce verification (NV):** If A believes X is fresh and A believes B once said X, then A believes B believes X.

$$\frac{A| \equiv (\#(X)), A| \equiv (B| \sim X)}{A| \equiv (B| \equiv X)} \quad (2)$$

- **Jurisdiction (JR):** If A believes B has jurisdiction over X and A believes B believes X, then A believes X.

$$\frac{A| \equiv (B \Longrightarrow X), A| \equiv (B| \equiv X)}{A| \equiv X} \quad (3)$$

- **Freshness meaning (FM):** The freshness rule states that any message with a fresh component is also fresh.

$$\frac{P| \equiv \#(X)}{P| \equiv \#(X, Y)}$$

If one part of a formula is fresh, then the entire formula must also be fresh.

- **Believe Rule (BR):** A principal believes a collection of statements i↵ he believes each component of the statements.

$$P| \equiv X, P| \equiv X$$
$$P| \equiv (X, Y)$$

- **Seeing Rule:** A principal sees all components of every message it sees, assuming it believes the necessary decryption key is a good key.

$$\frac{P \triangleleft (X,Y)}{P \quad X}, \qquad \frac{P \triangleleft \langle X \rangle_Y \quad P|\equiv (Q \leftrightarrow P)}{P \quad X}, \qquad \frac{\triangleleft \{\quad\}^K, P}{X_K}$$

C C C

Idealization

Idealization tries to turn the message sent into its intended semantics. It is a proceedure to get from protocol steps to logical inferences. A message in the idealized protocol is a formula. Given the protocol step:

$A \,!\, B : \{A, K_{ab}\} bs$ (4)

A sends to B, who uses his secret key K_{bs} to unlock the message $\{A, K_{ab}\}$ wich contains the key K_{ab} to be used in communicating between them. This can be expressed in idealized form as:

Kab

$A \,!\, B : \{A \,!\, B\} bs$ (5)

B knows the key K_{bs} and A and B communicates through the shared key K_{ab}. Idealized messages re of the form: $\{X\}K_1, \{X\}K_2, \cdots, \{X\}K_n$.

In BAN logic, idealization is meant to omit parts of the message that do not contribute to the beliefs of the recipients. In BAN all plaintext is omitted since it can be forged.

The Authentication Protocol

The goal of an authentication protool is to make a belief that the communication is carried out between trusted parties only. This is only achieved if the autghentication is based on a session key established between the server and the user. Thus authentication is deemed complete if there established a session key K thats used between A and B such that:

$A| \equiv (A \,!K\, B), \quad B| \equiv (A \,!K\, B)$

In some protocols, a deeper believe is achieved:

$A| \equiv B| \equiv (A \,!K\, B), \quad B| \equiv A| \equiv (A \,!K\, B)$

We presume a three factor based mutual authentication protocol in a multi-server environment. The presumed protocol consists of the following phases: initialization, registration, authentication and key agreement and password update phases. The notations used are as given in Table 1.

Table 1: Notations

Symbol	Description
RC	Registration Center
Ui, Sj	Users *i* & Server *j*
ID_i, PW_i	Identity and password for user *i*
n*1*,n*2*,a*1*,a*2*	Random numbers for each session
PubUi, PubSj	Public key for user *i* and server *j*
PriUi, PriSj	Private key for user *i* and server *j*
SK	Legitimate user session key

T_i	Time stamp

- **Initialization Phase:** RC initializes the system based on the design of the protocol.
- **Registration Phase:** User *i*, (U_i) and server *j*, (S_j) are issued with secret credentials and private key by the *RC*.
- **Server Registration Phase:** S_j registers to *RC* for mutual authentication with users registered in the system.
- **Authentication and Key Agreement Phase:** U_i and S_j execute authentication with each entity and compute a shared session key (*SK*).
- **Password Update Phase:** U_i enters his old credentials ID_i and password PW_i, if they are confirmed to be genuine, he is prompted to select PW^{New} and then the computing device makes the necessary computations and update the password to PW^{New}.

For a detailed decription of such an authentication protocol, please refer to (Sudhakar, Natarajan, Gopinath, & Saranyadevi, 2020).

Protocol Analysis

Asume an arbitrary authentication protocol that uses multi-servers. Let the following table define all the notations used.

BAN - Security Analysis

We will use the modal operators and logic rules defined above. In this protocol, the messages transmitted in the authentication and key agreement phase are $\{M_2, M_3, M_5, T_1\}$ and $\{M_7, M_8, T_2\}$.

- **Assumptions:** Let the assumptions of the protocol be as follows:
  - **AS-1:** $S_j \mid \equiv U_i \overset{a1}{\leftrightarrow} S_j$ – **AS-2:** $S_j \mid \equiv \#(T_1)$
  - **AS-3:** $U_i \mid \equiv U_i \overset{a2}{\leftrightarrow} S_j$
  - **AS-4:** $U_i \mid \equiv \#(T_2)$
  - **AS-5:** $S_j \mid \equiv U_i) (U_i \overset{SK}{\leftrightarrow} S_j)$
  - **AS-5:** $U_i \mid \equiv S_j) (U_i \overset{SK}{\leftrightarrow} S_j)$
- **Goals:** The following are main goals of the protocol.
  - **Goal - 1:** $U_i \mid \equiv (U_i \overset{SK}{\leftrightarrow} S_j)$ – **Goal - 2:** $S_j \mid \equiv (U_i \overset{SK}{\leftrightarrow} S_j)$
  - **Goal - 3:** $U_i \mid \equiv S_j \mid \equiv (U_i \overset{SK}{\leftrightarrow} S_j)$
  - **Goal - 4:** $S_j \mid \equiv U_i \mid \equiv (U_i \overset{SK}{\leftrightarrow} S_j)$
- **Idealized Form:** Assuming that in the protocol, two messages were exchanged between the user and the server over a public channel. The idealized form of the exchanged messagws are:
  - **Message - 1:** $U_i \; S_j : \{M_2, M_3, T_1\} a_1$
  - **Message - 1:** $S_j \; U_i : \{M_7, T_2\} a_2$
- **The BAN Logic Proof:**
  - **Step - 1:** We can derive S_1 from Message-1 $S_1 : S_j \mathrm{C} \{M_2, M_3, T_1\}$
  - **Step - 2:** We can derive S_2 from S_1 and AS_1 with MM. $S_2 : S_j \mid \equiv U_i \mid \leftarrow\cdots (M_2, M_3, T_1)$
  - **Step - 3:** We can derive S_3 from S_2 and AS_2 with FM. $S_3 : S_j \mid \equiv \#(M_2, M_3, T_1)$

- **Step - 4:** We can derive S_4 from S_2 and S_3 with NV. $S_4 : S_j | \between U_i | \between (M_2, M_3, T_1)$
- **Step - 5:** We can derive S_5 from Message - 2. $S_5 : U_i$ C $\{M_7, T_2\}$
- **Step - 6:** We can derive S_6 from S_5 and AS_3 with MM. $S_6 : U_i | \between S_j | \dashleftarrow (M_7, T_2)$
- **Step - 7:** We can derive S_7 from S_6 and AS_4 with FR. $S_7 : U_i | \between \#(M_7, T_2)$
- **Step - 8:** We can derive S_8 from S_6 and S_7 NV. $S_8 : U_i | \between S_j | \between (M_7, T_2)$
- **Step - 9:** We can derive S_9 from S_4. $S_9 : S_j | \between U_i | \between (U_i \,!^{SK}\, S_j)$ S_j calculates the session SK and thus **Goal 4** is achieved.
- **Step - 10:** We can derive S_{10} from S_8. $S_{10} : U_i | \between S_j | \between (U_i \,!^{SK}\, S_j)$. Where U_i calculates the session key SK, and hence **Goal 3** is achieved.
- **Step 11:** We can derive S_{11} from S_9 and AS_5. $S_{11} : S_j | \between (U_i \,!^{SK}\, S_j)$. **Goal 2** is achieved.
- **Step - 12:** We can derive S_{12} from S_{10} and AS_6. $S_{12} : U_i | \between (U_i \,!^{SK}\, S_j)$. **Goal 1** is achieved.

Conclusion

Based on the formal descriptions of cryptographic protocols using logic reasoning. We verify the semantic security of the session key and mutual authentication of an authentication protocol in a multi-server environment using BAN logic. Even though the logic and semantics has been elaborated, the notion of perfect secrecy has been relaxed in our considerion of the security of the protocol.

References

Abadi, M., & Tuttle, M. R. (1991). A semantics for a logic of authentication. In *Proceedings of the tenth annual acm symposium on principles of distributed computing* (pp. 201–216).

Ali, Z., Ghani, A., Khan, I., Chaudhry, S. A., Islam, S. H., & Giri, D. (2020). A robust authentication and access control protocol for securing wireless healthcare sensor networks. *Journal of Information Security and Applications*, *52*, 102502.

Boonkrong, S. (2021). Authentication and key establishment protocols. In *Authentication and access control* (pp. 163–195). Springer.

Burrows, M., Abadi, M., & Needham, R. (1990). A logic of authentication. *ACM Transactions on Computer Systems (TOCS)*, *8*(1), 18–36.

Fakroon, M., Alshahrani, M., Gebali, F., & Traore, I. (2020). Secure remote anonymous user authentication scheme for smart home environment. *Internet of Things*, *9*, 100158.

Harbi, Y., Aliouat, Z., Refoufi, A., Harous, S., & Bentaleb, A. (2019). Enhanced authentication and key management scheme for securing data transmission in the internet of things. *Ad Hoc Networks*, *94*, 101948.

Hassan, A., Omala, A. A., Ali, M., Jin, C., & Li, F. (2019). Identity-based user authenticated key agreement protocol for multi-server environment with anonymity. *Mobile Networks and Applications*, *24*(3), 890–902.

Miller, S. P., Neuman, B. C., Schiller, J. I., & Saltzer, J. H. (1988). Kerberos authentication and authorization system. In *In project athena technical plan.*

Mo, J., Hu, Z., Chen, H., & Shen, W. (2019). An e cient and provably secure anonymous user authentication and key agreement for mobile cloud computing. *Wireless Communications and Mobile Computing*, *2019*.

Mwitende, G., Ali, I., Eltayieb, N., Wang, B., & Li, F. (2020). Authenticated key agreement for blockchain-based wban. *Telecommunication Systems*, *74*(3), 347–365.

Needham, R. M., & Schroeder, M. D. (1978). Using encryption for authentication in large networks of computers. *Communications of the ACM*, *21*(12), 993–999.

Ostad-Sharif, A., Abbasinezhad-Mood, D., & Nikooghadam, M. (2019). An enhanced anonymous and unlinkable user authentication and key agreement protocol for tmis by utilization of ecc. *International journal of communication systems*, *32*(5), e3913.

Satyanarayanan, M. (1989). Integrating security in a large distributed system. *ACM Transactions on Computer Systems (TOCS)*, *7*(3), 247–280.

Sudhakar, T., Natarajan, V., Gopinath, M., & Saranyadevi, J. (2020). An enhanced authentication protocol for multi-server environment using password and smart card. *Wireless Personal Communications*, *115*(4), 2779–2803.

Ying, B., & Nayak, A. (2019). Lightweight remote user authentication protocol for multi-server 5g networks using self-certified public key cryptography. *Journal of Network and Computer Applications*, *131*, 66–74.

Zhang, Y., Xie, K., & Ruan, O. (2019). An improved and e cient mutual authentication scheme for session initiation protocol. *PloS one*, *14*(3), e0213688.